

**Conférence Benelux “Cybersecurity”
Maastricht, 5 avril 2011**

Intervention de Monsieur le Ministre François Biltgen

- Dear Ivo (Opstelten),

Dear Stefaan (De Clerck),

Dear Secretary-General Laarhoven,

Dear colleagues.

Thank you to the Netherlands for the initiative and organization of this conference about cybersecurity. There could probably be no better moment to meet and discuss these very important issues. I am happy we are bringing together all our experts for – I am sure – a fruitful discussion and laying the base for further cooperation. Already *now* I know that all of us will go back home *inspired*.

- We are three countries that are at the forefront of new technologies, we are IT-countries if I may call us like that. Among the three of us, we are at the top of the highest broadband penetration rates in the EU, we have strong and vibrant ICT-, new media- and IT-sectors and we are all actively promoting research in these new technologies – as we see today from the numerous representatives from the scientific and academic sectors. Of course, every country has its own focus, its own priorities. But I believe we are complementary in our efforts. And this is also what we should be seeking in this

dossier: complementarity, and above all: coordination – avoiding duplication of efforts and parallel planning. What we need – at all levels – is to establish a constant dialogue and exchange of information for further cooperation. So let's start!

- As you have already mentioned, and we agree on the premises here, Internet, ICT and new technologies are omnipresent in our world. They bring to us many benefits [think of electronic commerce, distant learning or real-time world-wide mobile communications], they make our lives easier – maybe sometimes more stressful! – and the entire world is just a mouse click away. Our lives – professional and private - can not be imagined without them anymore. We all agree on this.
- But the risks for disruption and abuse are also real. Our economy and society are increasingly dependent on what is now considered vital infrastructure. We are vulnerable via this all-pervasive network. We can think of accidental informatic crashes, of voluntary malicious attacks on networks and systems, or of criminal activities online. Cybersecurity, and cybercrime, cyberattacks – we need to brace ourselves against the risks involved. It is therefore elementary, necessary, essential, that we do everything to protect the infrastructure, to anticipate, prevent and analyse potential risks, and

of course, in the worst case scenario, to remedy and combat such incidents. As Minister of Justice, I consider it important that the ongoing negotiations on the EU's criminal law framework bring added value in comparison to the existing rules.

- This effort starts at the lowest level: the end-user and his laptop or mobile phone. It is both about the way the user *behaves* online, but also about the software protecting the private *terminal*. In Luxembourg, we are very active with awareness raising campaigns, and focus particularly on schools since young people are especially concerned. Although – I admit – they are also probably the ones that are most knowledgeable when it comes to the new technologies and online services. More than our generation maybe! [I see it when I look at my children ...]
- The next level up is the professional sector, both public and private. We need to make sure that all economic actors, and our own administrations, are sufficiently resilient and have the necessary means at their disposal to react efficiently in case of a threat. As you said, Ivo [and Stefaan], government and business need to work together. We, government, depend on the expertise and know-how of the private sector. In return, business needs the public administration to flourish and in coordination efforts across the

economy. In that sense, I am proud to have all sectors from Luxembourg represented today in Maastricht. Luxembourg is indeed active in this field, thanks to the Ministry of the Economy, and is bringing together public and private actors, for their mutual benefit and establishing trust. You will be able to gain insight into the operational collaboration between the public and private sector in Luxembourg in one of our workshops this afternoon. The focus will be specifically on SMEs who sometimes have the most difficulties or are least aware of the necessity for implementing information security measures. What seems obvious is that these activities are “donnant-donnant” for all involved: private actors – both the supplier of the security application and the customer receiving it - and the public sector ultimately benefitting from a more secure IT environment.

- In complement to this, there is the crucial element of research. Research allows for *developing* the necessary methods for anticipating and detecting risks and threats. And I am proud to highlight the activities of the Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg. Our experts will demonstrate some of their cutting-edge research – both applied and academic – in their workshop this afternoon and present a

couple of showcases during lunch later on (one of them appropriately called “honeypot”!).

- And then, we need to bring all of this together at national level! There is a strong need for coherence, for organization and for coordination. As I already told you at our Benelux breakfast before the last JAI-Council, we are currently fine-tuning our national strategy to take up these challenges. Politically, the challenge is to get all concerned ministers on the same page: amongst others, the minister for Communications, the minister for Justice, the minister for Public Administration, the minister for Research and Higher Education, but also the ministry of State, the ministry of the Economy and the ministry of Education need to be involved. This is not a big problem in Luxembourg, luckily, since I combine many of these portfolios and will mainly have to discuss and agree with myself!
- In this perspective, I underline again that the conference today is very useful for all of us, as everyone will learn from the other’s experiences and take them home to bring forward our own plans. I would also like to underline that I am proud of the impressive array of representatives from all concerned sectors in Luxembourg present today in Maastricht, showing that we have already a very active,

competent and open community in place. There are some sectors that are in particular need of highly secure and reliable networks, infrastructures and data vaults- and that is why I am looking forward to hearing what M Jean Hilger will have to say to us in just a moment, giving us the financial sector perspective. I think this is highly relevant for our three countries.

- But we are here to go beyond the national challenge of addressing these issues. The bigger challenge is the cross-border aspect: we need to cooperate across borders! Otherwise all our national efforts are a waste of time. The theme of today's conference is thus well chosen: "Success through cooperation". The interlinked digital world does not take into consideration national borders. We need to work together, at all levels: technical, expert, researcher, public, private, political. The Luxembourg expert needs to know who his/her "vis-à-vis" is, who his/her counterpart in the Netherlands and in Belgium is. Beyond this practical cooperation, I believe we need a common vision. And I think today we are sending a very clear message in this respect and it is an *honour* and *pleasure* for me to support and sign the Declaration of Intent. The Benelux dimension is an integral part of our cybersecurity efforts and our cooperation allows us to "top-up", to improve the national measures already in place.

- Although I think this is a premiere of regional cooperation in the field of cybersecurity, we cannot stop our efforts at Benelux borders either. And I am not revealing a secret when I say that it is not the first time that from a Benelux initiative something bigger has followed. We are building a model for cooperation between countries that can serve as an example to others and can be transposed at a larger scale: at European level. As you know, there are many initiatives in this field at EU level. All these initiatives need to be coherent. We, as Benelux countries, can make sure this happens and bring in our full weight to support further coordination EU-wide. In that sense I believe that today's initiative should also be reflected in the forthcoming events organized by the Hungarian Presidency [for example the Ministerial Conference in Balatonfüred or the Ministerial Conference in Budapest].
- Benelux and the EU – both levels cannot make abstraction from the global dimension. National, regional and European activities do not take place in a vacuum. We all know that. We need to look for a regular dialogue with partners across the world, preferably in a multilateral context (there are activities going on in the OECD and the UN as well). Cybersecurity is a truly global challenge, and *everybody* needs to pull their weight. Which is what *we* are doing

today. National and regional initiatives – such as today’s Benelux meeting – are vital – I dare say, necessary – elements in putting in place successful European and international cooperation structures. And that is why I believe that we are today if not laying the grounds then constituting a solid building block in the underpinning of EU and global cybersecurity coordination.

- Thank you again for the invitation and organization, and I wish us all a very fruitful and lively exchange this afternoon.
